

电站控制系统网络安全攻击研究

中国东方电气集团中央研究院 袁晓舒

求实 创新 人和 图强



1

中国东方电气集团简介

2

拒绝服务攻击对电站控制系统危害

3

现场总线攻击对电站控制系统危害

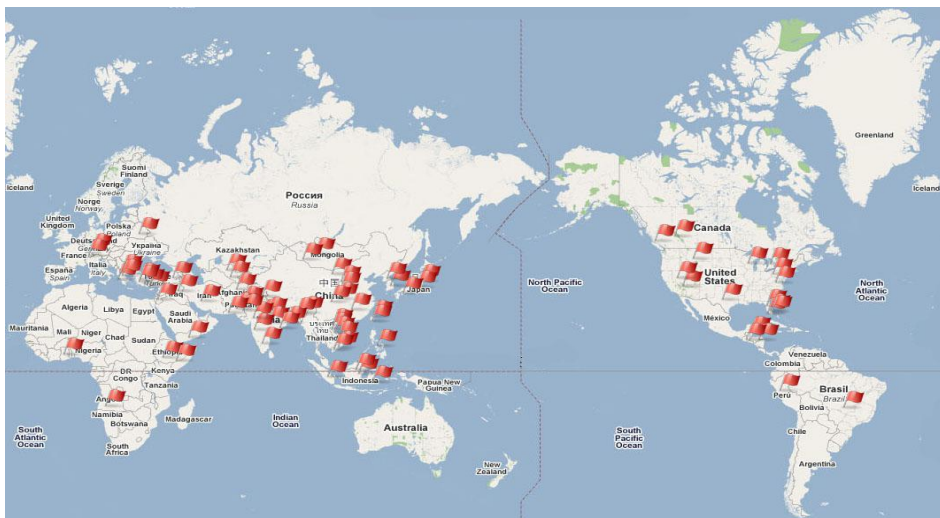
4

总结

求实 创新 人和 图强



中国东方电气集团有限公司（简称“东方电气”）是党中央、国务院确定的“涉及国家安全和国民经济命脉的国有重要骨干企业”之一，中国最大的发电设备制造、电站工程承包及机电成套设备出口基地之一，属国务院国资委监管国有独资企业。



- 水电 单机最大1000MW等级系列水轮发电机组
- 火电 单机最大1200MW等级系列火电机组
- 核电 单机最大1700MW等级第三代核电机组主设备
- 燃气发电 E/F级重型燃气轮机
- 风电 单机最大5.5MW等级系列风电机组
- 太阳能发电 100MW级太阳能光热电站、光伏发电站
- 环保 烟气污染物处理、余热锅炉、高效电机等
- 海水淡化 单体最大每日12500吨级海水淡化设备
- 电力电子 大功率变频器、发电装备控制系统、电站DCS控制

系统等电力电子产品

火电



DCS、锅炉控制、汽机控制、发电机控制、水处理控制系统、煤处理控制、灰浆处理控制、脱硝处理控制等。

水电



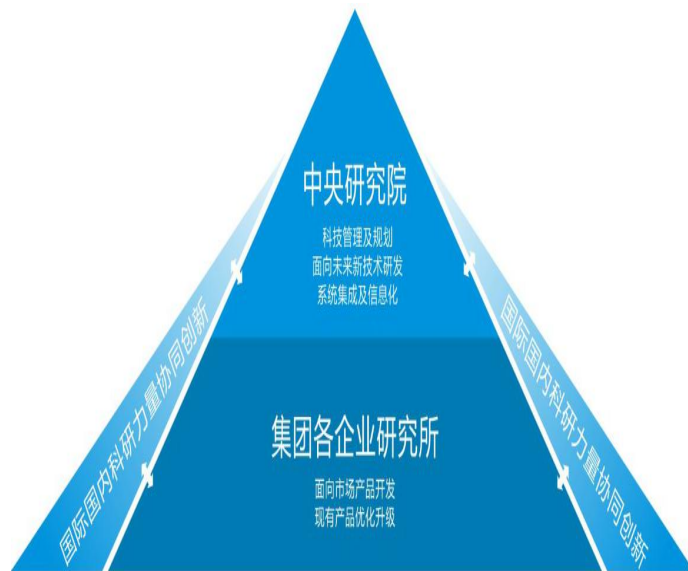
DCS、水轮机控制系统、发电机控制系统、水电厂自动化系统、发电机静态变频启动系统（**SFC**）等。

风电



电场**SCADA**、风机主控系统、变桨控制系统、偏航控制系统、风电变流器、风机振动分析系统、风机消防系统、风机视频监控系统。

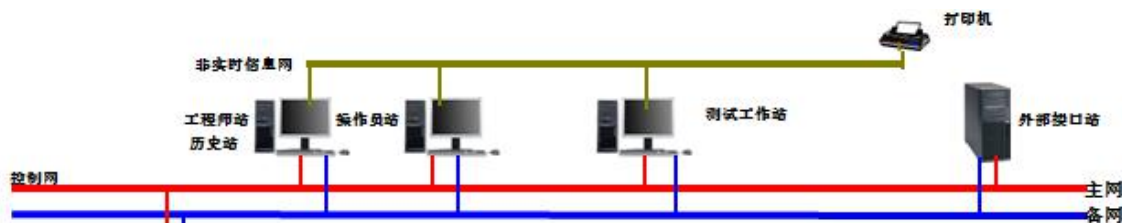
- **面向未来：** 智能装备及制造、电力电子、超导技术、新能源汽车动力总成、先进能源转换技术、清洁燃烧技术、储能技术、太阳能发电技术、新能源系统集成技术；
- **面向企业：** 共性技术研究、核心技术攻关、智能制造、信息化建设；
- **面向工程：** 电站工程设计、新能源系统设计研究、EPC工程支持及咨询、环保工程设计咨询。



- 1 中国东方电气集团简介
- 2 拒绝服务攻击对电站控制系统危害
- 3 现场总线攻击对电站控制系统危害
- 4 总结

求实 创新 人和 图强





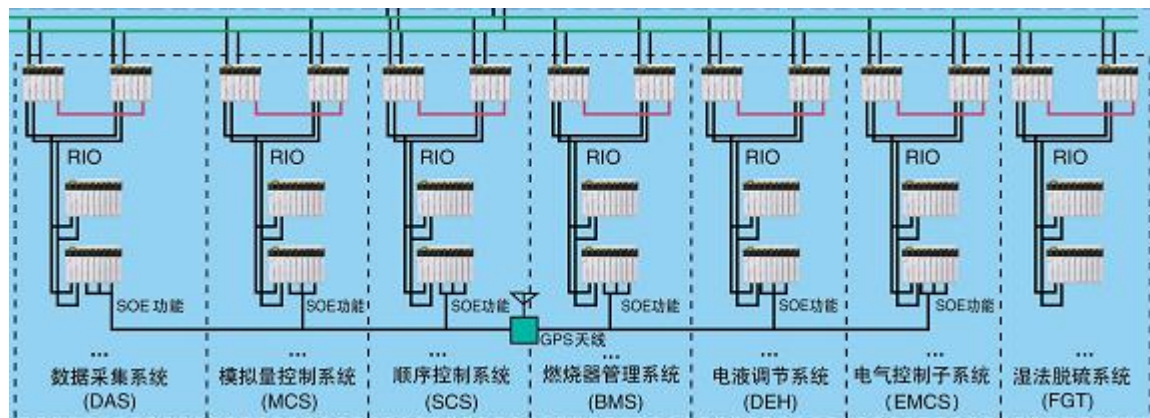
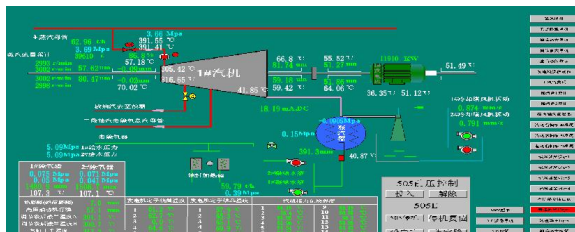
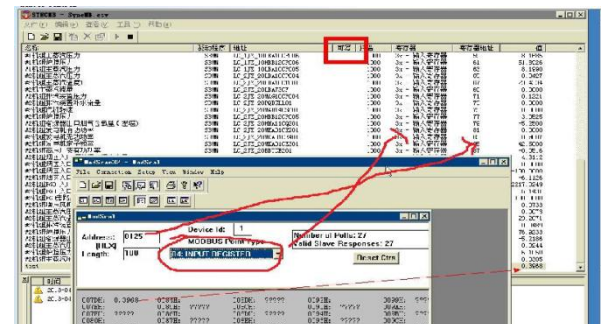
示波器

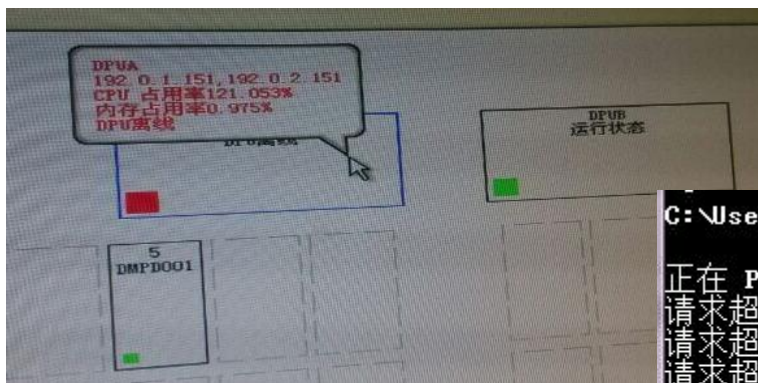
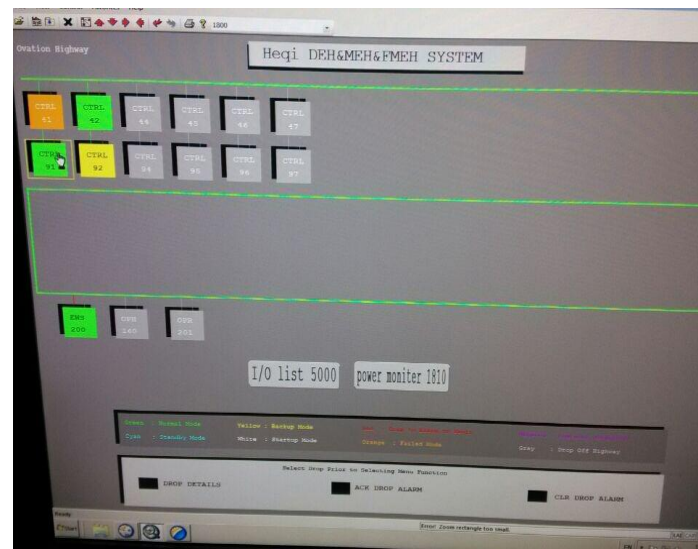
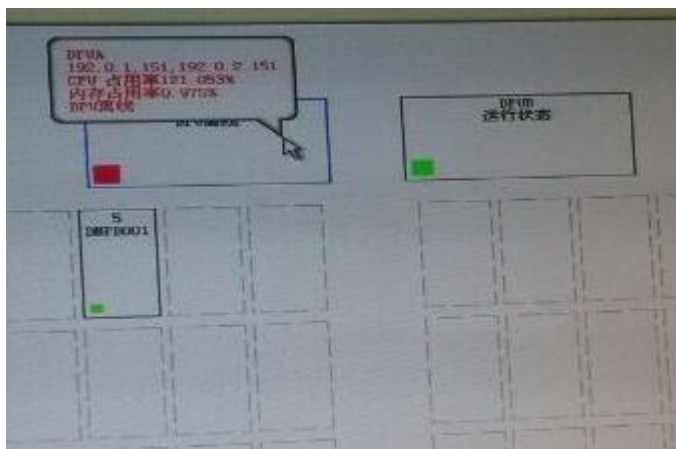


信号发生器



万用表





```
C:\Users\Administrator>ping 192.168.2.41
```

```
正在 Ping 192.168.2.41 具有 32 字节的数据:  
请求超时。  
请求超时。  
请求超时。  
请求超时。
```

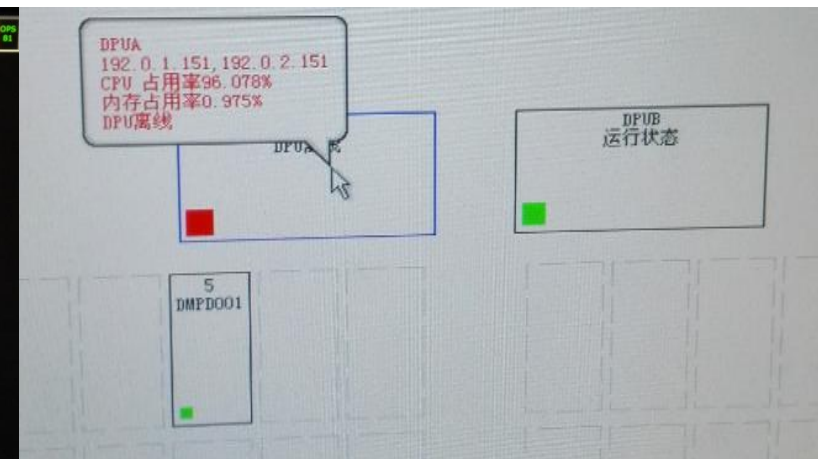
```
192.168.2.41 的 Ping 统计信息:
```

```
数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```

```

13:15:42.315422 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:15:43.315275 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:15:45.315057 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:15:46.318785 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:15:47.316864 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:15:48.321212 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:15:49.326372 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:15:50.326221 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:15:51.326871 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:15:52.319829 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:15:53.319708 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:15:54.319636 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:15:56.323429 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:15:57.323188 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:15:58.323848 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:15:59.322897 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:16:00.322751 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:16:01.322598 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:16:02.322462 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:16:03.322338 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:16:04.322164 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:16:05.322027 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:16:07.321811 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:16:08.321656 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:16:09.321436 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:16:10.321278 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:16:11.321131 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:16:12.320979 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:16:13.320831 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:16:14.320681 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:16:15.320549 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:16:16.320392 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:16:18.320221 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:16:19.319945 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:16:20.319799 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:16:21.319652 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:16:22.319511 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46
13:16:23.319355 ARP, Request who-has 192.0.1.131 tell 192.0.1.132, length 46

```





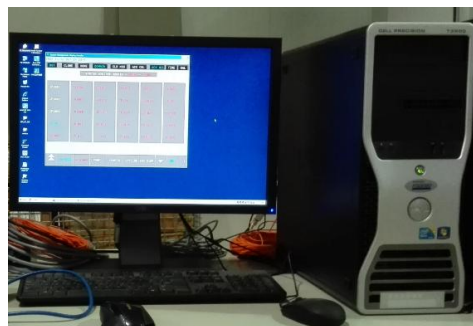
- 100

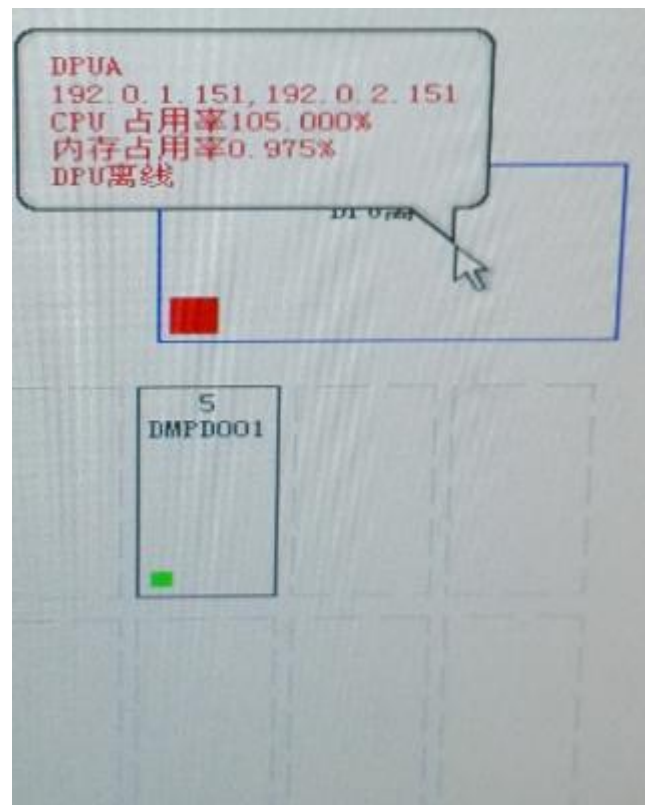
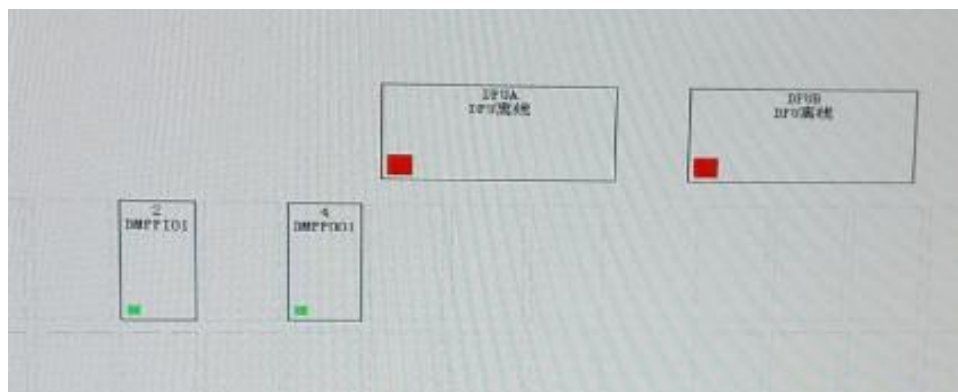
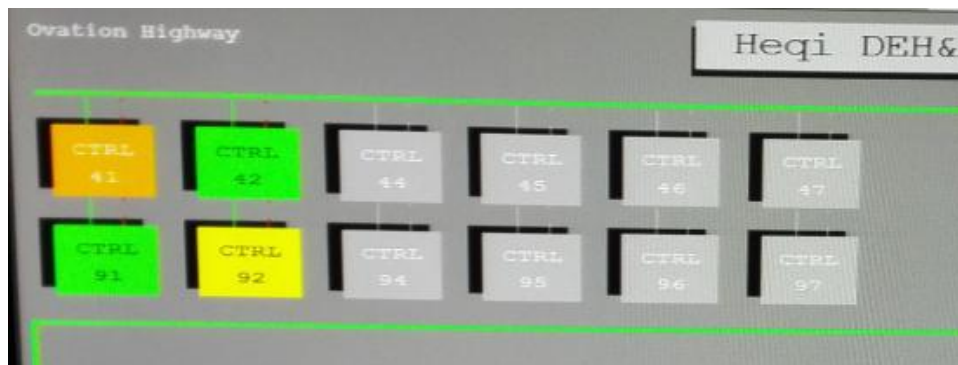


- 1 中国东方电气集团简介
- 2 拒绝服务攻击对电站控制系统危害
- 3 现场总线攻击对电站控制系统危害**
- 5 总结

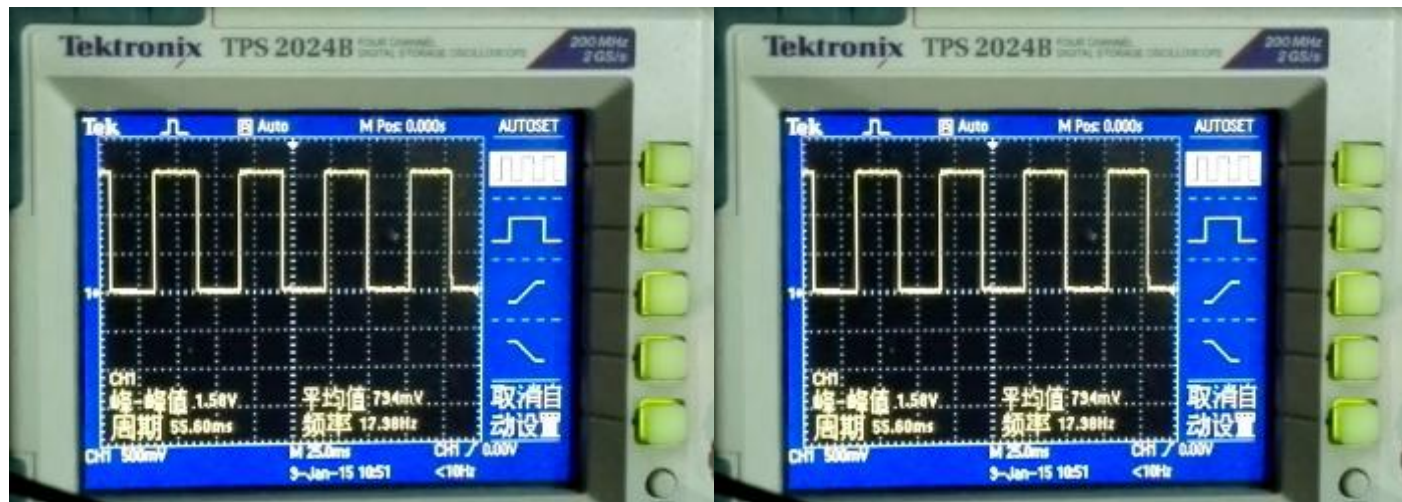
求实 创新 人和 图强

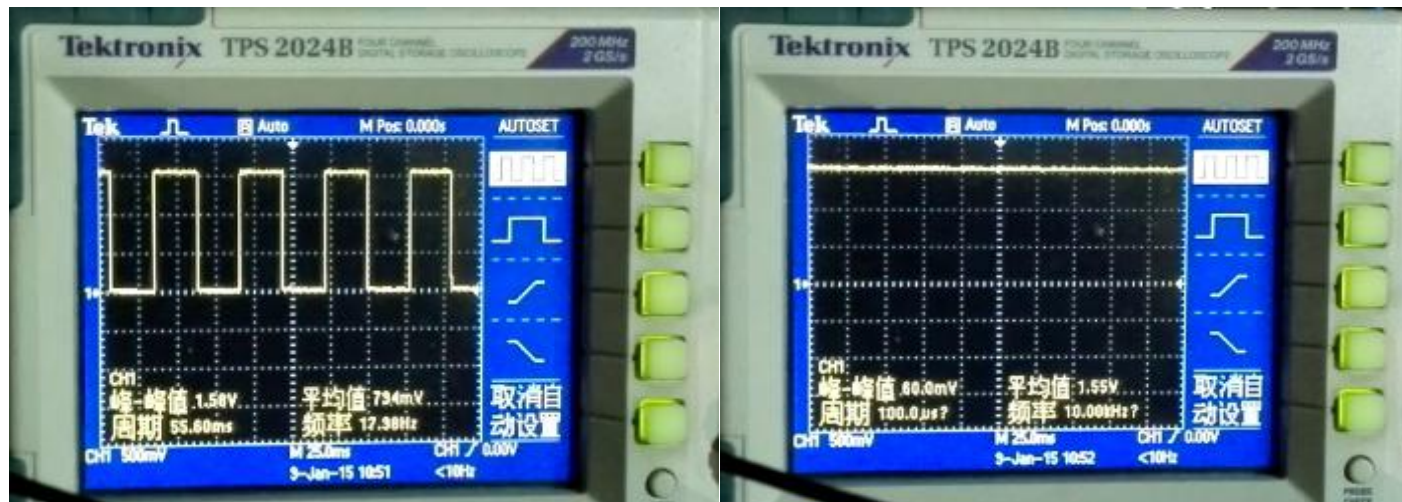


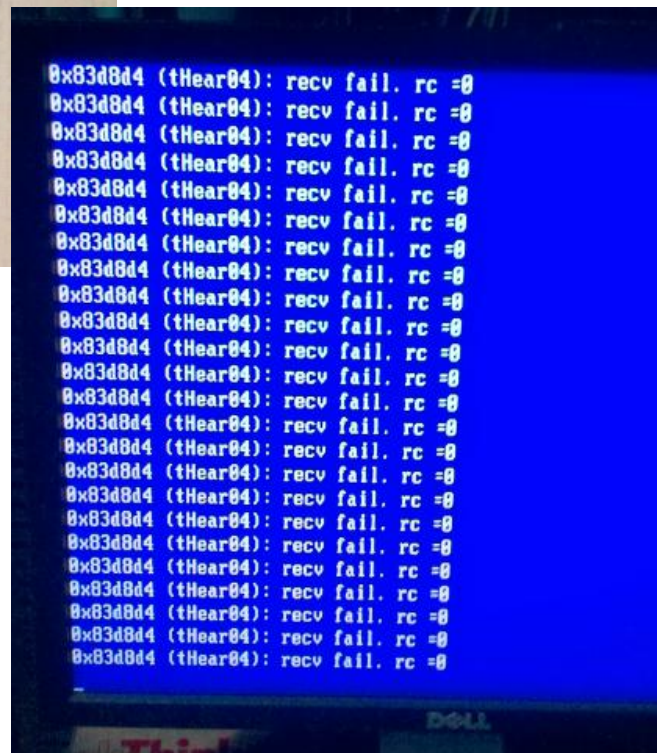
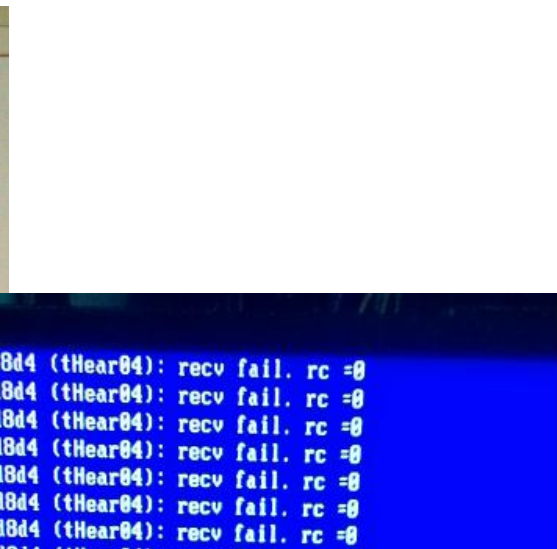




```
-> 0x83d7cc (tHear04): recv fail. rc =0  
0x916488 (tDebug): SuspendTasksForReload  
0x916488 (tDebug): ResumeTasksForReload
```







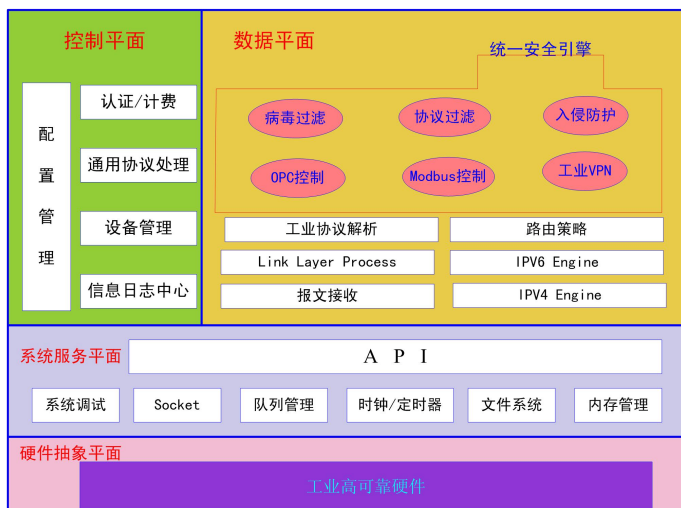
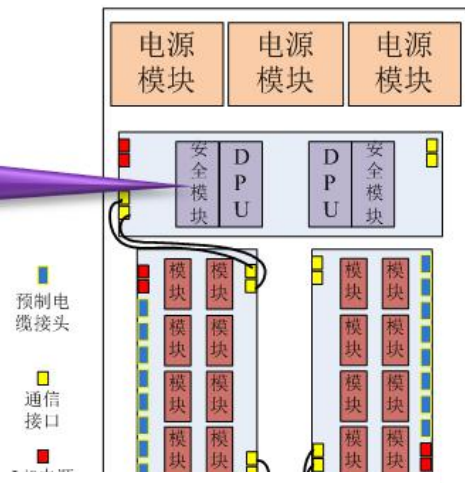
- 1 中国东方电气集团简介
- 2 拒绝服务攻击对电站控制系统危害
- 3 现场总线攻击对电站控制系统危害
- 4 总结

求实 创新 人和 图强





**安全
防护模块**





RichData
大数据智能分析平台

数据源 数据清洗 数据集成 数据仓库 数据可视化 数据应用

数据源 数据清洗 数据集成 数据仓库 数据可视化 数据应用

■ 诊断报告



以信息安全提升产品价值。

谢谢

